

# MULTI-MEDIA DATA DISTRIBUTION SYSTEM AND MULTI-MEDIA DATA REPRODUCTION TERMINAL

**Publication number:** JP10333769

**Publication date:** 1998-12-18

**Inventor:** IWAMA KENJI; NAGASHIMA NORIMITSU

**Applicant:** MITSUBISHI ELECTRIC CORP

**Classification:**

- international: **G06F1/00; G06F15/00; G06F21/00; G10K15/02; H04L9/32; H04M3/42; H04M11/08; H04M15/00; H04N7/16; H04N7/173; G06F1/00; G06F15/00; G06F21/00; G10K15/02; H04L9/32; H04M3/42; H04M11/08; H04M15/00; H04N7/16; H04N7/173; (IPC1-7): G06F1/00; G06F15/00; H04L9/32; H04M3/42; H04M11/08; H04M15/00; H04N7/16**

- european:

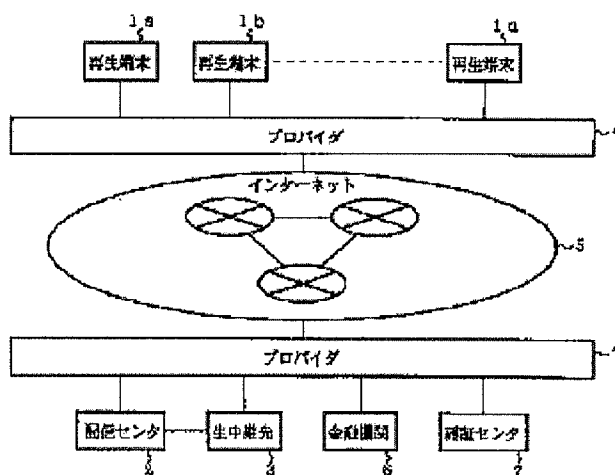
**Application number:** JP19970145635 19970603

**Priority number(s):** JP19970145635 19970603

Report a data error here

## Abstract of JP10333769

**PROBLEM TO BE SOLVED:** To allow a user to receive the service of truly desired high quality data at a proper charge. **SOLUTION:** A reproducing terminal 1a transmits the identification information and certification information of prescribed data to a distributing center 2. The distributing center 2 checks the transmitted certification information, operates a charging processing, instructs a financial institution 6 to collect the charge, and distributes data corresponding to the identification information and additional information for extinguishing the data after reproduction to the reproducing terminal 1a. The reproducing terminal 1a reproduces the data, and extinguishes the data.



Data supplied from the **esp@cenet** database - Worldwide

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-333769

(43) 公開日 平成10年(1998)12月18日

(51) Int.Cl. <sup>6</sup>	識別記号	F I
G 0 6 F 1/00	3 7 0	C 0 6 F 1/00 3 7 0 F
15/00	3 3 0	15/00 3 3 0 Z
H 0 4 L 9/32		H 0 4 M 3/42 Z
H 0 4 M 3/42		11/08
11/08		15/00 Z

審査請求 未請求 請求項の数11 O L (全 10 頁) 最終頁に続く

(21) 出願番号 特願平9-145635

(22) 出願日 平成9年(1997)6月3日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 岩間 研二

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 永島 規充

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

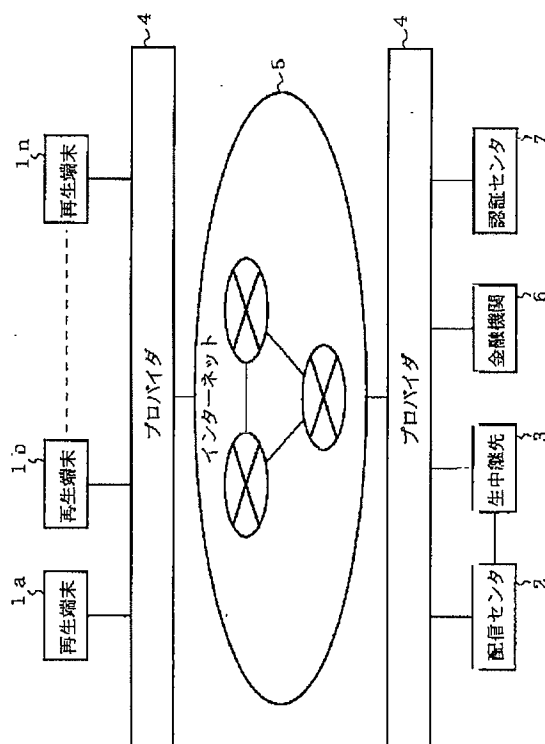
(74) 代理人 弁理士 田澤 博昭 (外1名)

(54) 【発明の名称】 マルチメディアデータ配信システム及びマルチメディアデータ再生端末

## (57) 【要約】

【課題】 ユーザが真に欲しい高品質のデータを適正な価格で入手することが困難であった。またサービス提供会社にとってみれば、インターネットを介しての確実なデータ要求者の特定、課金及び料金回収システムに課題があった。

【解決手段】 再生端末1aは、所定のデータの識別情報と認証情報とを配信センタ2に送信する。配信センタ2は送信された認証情報をチェックし、課金処理を行って金融機関6に料金回収の指示を行うと共に、識別情報に対応したデータと再生後にこのデータを消滅させる付加情報とを再生端末1aに配信する。再生端末1aはデータを再生後にデータを消滅させる。



**【特許請求の範囲】**

【請求項1】 所定のマルチメディアデータの配信要求を行い、配信されたマルチメディアデータを再生する再生端末と、

複数のマルチメディアデータを保有し、上記再生端末からの配信要求に基づきマルチメディアデータを配信すると共に、上記再生端末への課金処理を行う配信センタと、

上記配信センタの課金処理に基づき、上記再生端末に対し料金回収を行う金融機関と、

上記再生端末、上記配信センタ及び上記金融機関と上記マルチメディアデータの配信に係わる加入契約を結び、配信サービスを提供するプロバイダと、

上記加入契約に基づき、上記再生端末の認証情報を管理する認証センタとを備え、

上記再生端末は、上記所定のマルチメディアデータの識別情報を含んだ配信要求情報と、上記認証センタにより管理されている認証情報とを、上記配信センタに送信し、

上記配信センタは、上記再生端末から送信された認証情報と上記認証センタにより管理されている認証情報とを比較することにより上記プロバイダと加入契約を結んだ再生端末であることを確認し、上記再生端末から送信された配信要求情報と認証情報に基づき、上記再生端末への課金処理を行って上記金融機関に料金回収の指示を行うと共に、上記配信要求情報に対応するマルチメディアデータと再生後にこのマルチメディアデータを消滅させる付加情報とを含んだ配信情報を上記再生端末に配信し、

上記再生端末は上記配信情報を受信し、上記配信センタから配信されたマルチメディアデータを再生すると共に、上記付加情報に基づき上記マルチメディアデータを消滅させることを特徴とするマルチメディアデータ配信システム。

【請求項2】 プロバイダと契約し、マルチメディアデータを生中継する生中継先を備え、

配信センタは、再生端末からの配信要求に基づき、上記生中継先のマルチメディアデータを上記再生端末に配信することを特徴とする請求項1記載のマルチメディアデータ配信システム。

【請求項3】 再生端末は、配信要求情報にマルチメディアデータの再生回数を含めて、配信センタに送信し、上記配信センタは、上記再生端末から送信された配信要求情報と認証情報に基づき課金処理を行うと共に、上記配信情報に上記再生回数を含めて上記再生端末に配信し、

上記再生端末は、上記配信された再生回数に対応して、上記配信されたマルチメディアデータを再生することを特徴とする請求項1記載のマルチメディアデータ配信システム。

【請求項4】 再生端末は、配信要求情報と認証情報を暗号化して、配信センタに送信し、

上記配信センタは、上記暗号化された配信要求情報と認証情報を復号化すると共に、配信情報を暗号化して、上記再生端末に配信し、

上記再生端末は、上記暗号化された配信情報を復号化することを特徴とする請求項1から請求項3のうちのいずれか1項記載のマルチメディアデータ配信システム。

【請求項5】 認証センタは、再生端末及び配信センタに、公開鍵暗号方式で使用する鍵を配布し、

上記再生端末は、配信要求情報を所定の鍵Rを使用して秘密鍵暗号方式により暗号化し、認証情報と上記所定の鍵Rを、上記認証センタから配布された鍵を使用して、公開鍵暗号方式により暗号化して、上記配信センタに送信し、上記配信センタは、上記公開鍵暗号方式により暗号化された認証情報と所定の鍵Rを、上記認証センタから配布された鍵を使用して、公開鍵暗号方式により復号化し、上記秘密鍵暗号方式により暗号化された配信要求情報を、上記復号化された鍵Rを使用して秘密鍵暗号方式により復号化すると共に、上記配信情報を所定の鍵R'を使用して秘密鍵暗号方式により暗号化し、上記所定の鍵R'を、上記認証センタから配布された鍵を使用して、公開鍵暗号方式により暗号化して、上記再生端末に配信し、

上記再生端末は、上記公開鍵暗号方式により暗号化された所定の鍵R'を、上記認証センタから配布された鍵を使用して、公開鍵暗号方式により復号化し、上記秘密鍵暗号方式により暗号化された配信情報を、上記復号化された鍵R'を使用して秘密鍵暗号方式により復号化することを特徴とする請求項1から請求項3のうちのいずれか1項記載のマルチメディアデータ配信システム。

【請求項6】 再生端末は、認証情報に識別情報を圧縮した識別情報ダイジェストを含めて配信センタに送信し、

上記配信センタは、公開鍵暗号方式により復号化された識別情報ダイジェストと、秘密鍵暗号方式により復号化された識別情報を比較することを特徴とする請求項5記載のマルチメディアデータ配信システム。

【請求項7】 複数のマルチメディアデータを保有している配信センタへ所定のマルチメディアデータの配信要求を行い、所定のマルチメディアデータを受信して再生するマルチメディアデータ再生端末において、上記受信した所定のマルチメディアデータを記憶するデータ記憶手段と、

上記受信した所定のマルチメディアデータを再生するデータ再生手段と、

上記配信センタからの指示に基づき、上記データ再生手段で再生後、上記所定のマルチメディアデータを消滅させる消滅処理制御手段とを備えたことを特徴とするマルチメディアデータ再生端末。

【請求項8】 配信センタからの指示に基づき、データ再生手段における所定のマルチメディアデータの繰返し再生回数を制御する繰返し再生制御手段を備えたことを特徴とする請求項7記載のマルチメディアデータ再生端末。

【請求項9】 配信要求を暗号化すると共に、配信センタから配信された暗号化された所定のマルチメディアデータを復号化する暗号化／復号手段を備えたことを特徴とする請求項7または請求項8記載のマルチメディアデータ再生端末。

【請求項10】 暗号化／復号手段は、秘密鍵暗号方式と公開鍵暗号方式の併用により、暗号化及び復号化することを特徴とする請求項9記載のマルチメディアデータ再生端末。

【請求項11】 データ記憶手段、データ再生手段、消滅処理制御手段及び繰返し再生制御手段とを分解不可能な筐体に格納されることを特徴とする請求項8記載のマルチメディアデータ再生端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、音楽やビデオ等のマルチメディアデータをユーザの要求に応じ適正な価格で効率良く配信するマルチメディアデータ配信システム及びマルチメディアデータ再生端末に関するものである。

【0002】

【従来の技術】インターネットの普及に伴い、音楽やビデオ等のマルチメディアデータのサービス提供が盛んになりつつある。従来の技術として例えば特平8-503584号に示された「対話式マルチメディア娯楽システム」がある。これは複数の歌を記憶する手段と、この記憶手段から複数の歌の1つを選択する手段と、この選択手段にตอบสนองし、記憶手段から1つの歌を受信する手段とを備え、この受信手段は、記憶手段から1つの歌の料金に関する情報も受信し、1つの歌に対する演奏の回数を制限する手段を含んだものである。しかし一般に従来のデータサービスは、サービス提供を受けるユーザ及びサービス提供を行うサービス提供会社双方にとって満足のいくものではなかった。

【0003】

【発明が解決しようとする課題】ユーザにとってみれば、真に欲しい高品質のデータのみを適正な価格で入手することが困難であり、入手したデータのなかには欲しくないデータが含まれているという課題があった。また欲しいデータだけを入手できたとしても、その品質に満足が得られないことが多かった。例えばミュージックコンテンツとしての「通信カラオケ」は、コード化された音符データを少ない情報量でしか伝送していないため、本格的なH i - F i 音で音楽を楽しむことができない。またサービス提供会社にとってみれば、インターネット

を介しての確実なデータ要求者の特定、課金及び料金回収システムに課題があった。さらに、ユーザがインターネットを介してデータを要求したときに、要求した内容に関するデータ要求者のプライバシーに不安があるという課題があった。さらに、配信されたマルチメディアコンテンツの著作権の保護に課題があった。

【0004】この発明は上記のような課題を解決するためになされたもので、ユーザが真に欲しい高品質のデータを適正な料金でサービスを受けられるようにすることを目的とする。また、インターネットを介しての確実なデータ要求者の特定、課金及び料金回収を実現することを目的とする。さらに、マルチメディアデータ配信を要求したユーザのプライバシーを保護することを目的とする。さらに、インターネット上で配信されるマルチメディアコンテンツの著作権者を保護することを目的とする。

【0005】

【課題を解決するための手段】請求項1記載の発明に係るマルチメディアデータ配信システムは、所定のマルチメディアデータの配信要求を行い、配信されたマルチメディアデータを再生する再生端末と、複数のマルチメディアデータを保有し、上記再生端末からの配信要求に基づきマルチメディアデータを配信すると共に、上記再生端末への課金処理を行う配信センタと、上記配信センタの課金処理に基づき、上記再生端末に対し料金回収を行う金融機関と、上記再生端末、上記配信センタ及び上記金融機関と上記マルチメディアデータの配信に係わる加入契約を結び、配信サービスを提供するプロバイダと、上記加入契約に基づき、上記再生端末の認証情報を管理する認証センタとを備え、上記再生端末が、上記所定のマルチメディアデータの識別情報を含んだ配信要求情報と、上記認証センタにより管理されている認証情報とを、上記配信センタに送信し、上記配信センタが、上記再生端末から送信された認証情報と上記認証センタにより管理されている認証情報とを比較することにより上記プロバイダと加入契約を結んだ再生端末であることを確認し、上記再生端末から送信された配信要求情報と認証情報に基づき、上記再生端末への課金処理を行って上記金融機関に料金回収の指示を行うと共に、上記配信要求情報に対応するマルチメディアデータと再生後にこのマルチメディアデータを消滅させる付加情報とを含んだ配信情報を上記再生端末に配信し、上記再生端末が上記配信情報を受信し、上記配信センタから配信されたマルチメディアデータを再生すると共に、上記付加情報に基づき上記マルチメディアデータを消滅させるようにしたものである。

【0006】請求項2記載の発明に係るマルチメディアデータ配信システムは、プロバイダと契約し、マルチメディアデータを生中継する生中継先を備え、配信センタが、再生端末からの配信要求に基づき、上記生中継先の

マルチメディアデータを上記再生端末に配信するようにしたものである。

【0007】請求項3記載の発明に係るマルチメディアデータ配信システムは、再生端末が、配信要求情報にマルチメディアデータの再生回数を含めて、配信センタに送信し、上記配信センタが、上記再生端末から送信された配信要求情報と認証情報に基づき課金処理を行うと共に、配信情報に上記再生回数を含めて上記再生端末に配信し、上記再生端末が、上記配信された再生回数に対応して、上記配信されたマルチメディアデータを再生するようにしたものである。

【0008】請求項4記載の発明に係るマルチメディアデータ配信システムは、再生端末が、配信要求情報と認証情報を暗号化して、配信センタに送信し、上記配信センタが、暗号化された配信要求情報と認証情報を復号化すると共に、配信情報を暗号化して、上記再生端末に配信し、上記再生端末が、上記暗号化された配信情報を復号化するようにしたものである。

【0009】請求項5記載の発明に係るマルチメディアデータ配信システムは、認証センタが、再生端末及び配信センタに、公開鍵暗号方式で使用する鍵を配布し、上記再生端末が、配信要求情報を所定の鍵Rを使用して秘密鍵暗号方式により暗号化し、認証情報と上記所定の鍵Rを、上記認証センタから配布された鍵を使用して、公開鍵暗号方式により暗号化して、上記配信センタに送信し、上記配信センタが、上記公開鍵暗号方式により暗号化された認証情報と所定の鍵Rを、上記認証センタから配布された鍵を使用して、公開鍵暗号方式により復号化し、上記秘密鍵暗号方式により暗号化された配信要求情報を、上記復号化された鍵Rを使用して秘密鍵暗号方式により復号化すると共に、上記配信情報を所定の鍵R'を使用して秘密鍵暗号方式により暗号化し、上記所定の鍵R'を、上記認証センタから配布された鍵を使用して、公開鍵暗号方式により暗号化して、上記再生端末に配信し、上記再生端末が、上記公開鍵暗号方式により暗号化された所定の鍵R'を、上記認証センタから配布された鍵を使用して、公開鍵暗号方式により復号化し、上記秘密鍵暗号方式により暗号化された配信情報を、上記復号化された鍵R'を使用して秘密鍵暗号方式により復号化するようにしたものである。

【0010】請求項6記載の発明に係るマルチメディアデータ配信システムは、再生端末が、認証情報に識別情報を圧縮した識別情報ダイジェストを含めて配信センタに送信し、上記配信センタが、公開鍵暗号方式により復号化された識別情報ダイジェストと、秘密鍵暗号方式により復号化された識別情報を比較するようにしたものである。

【0011】請求項7記載の発明に係るマルチメディアデータ再生端末は、複数のマルチメディアデータを保有している配信センタへ所定のマルチメディアデータの配

信要求を行い、所定のマルチメディアデータを受信して再生するものにおいて、上記受信した所定のマルチメディアデータを記憶するデータ記憶手段と、上記受信した所定のマルチメディアデータを再生するデータ再生手段と、上記配信センタからの指示に基づき、上記データ再生手段で再生後、上記所定のマルチメディアデータを消滅させる消滅処理制御手段とを備えるようにしたものである。

【0012】請求項8記載の発明に係るマルチメディアデータ再生端末は、上記配信センタからの指示に基づき、データ再生手段における所定のマルチメディアデータの繰返し再生回数を制御する繰返し再生制御手段を備えるようにしたものである。

【0013】請求項9記載の発明に係るマルチメディアデータ再生端末は、上記配信要求を暗号化すると共に、配信センタから配信された暗号化された所定のマルチメディアデータを復号化する暗号化／復号手段を備えるようにしたものである。

【0014】請求項10記載の発明に係るマルチメディアデータ再生端末は、暗号化／復号手段が、秘密鍵暗号方式と公開鍵暗号方式の併用により、暗号化及び復号化するようにしたものである。

【0015】請求項11記載の発明に係るマルチメディアデータ再生端末は、データ記憶手段、データ再生手段、消滅処理制御手段及び繰返し再生制御手段とを分解不可能な筐体に格納されるようにしたものである。

【0016】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態1. 図1はこの発明の実施の形態1によるマルチメディアデータ配信システムを示す構成図であり、図において、1a, 1b, ... 1nは、デジタル情報等のマルチメディアデータの配信要求を行い、送信されたマルチメディアデータを受信し再生する再生端末、2はデジタル情報としてのマルチメディアデータを保有し、上記再生端末1a, 1b, ... 1nからのマルチメディアデータの配信要求を受け配信すると共に、課金処理を行う配信センタ、3は配信センタの管理下であり生中継を行う生中継先、4はインターネット5を介し上記再生端末1a, 1b, ... 1nに配信センタ2からのマルチメディアデータの配信サービスを提供するプロバイダ、6は上記配信センタ2の課金処理に基づき、マルチメディアデータを利用した再生端末に対し、料金回収を行う金融機関、7は上記プロバイダに加入している上記再生端末1a, 1b, ... 1n、配信センタ2、生中継先3及び金融機関6を特定する認証センタである。

【0017】上記再生端末1a, 1b, ... 1n、配信センタ2、生中継先3及び金融機関6は、プロバイダ4と加入契約を結んだ者だけが利用できる。そしてその

管理は認証センタ7が行い、利用しようとする者を必ず特定することができる。

【0018】配信センタ2は、例えば音楽、ビデオ、コンピューティングサービス等の提供を行うデジタルコンテンツ配信センタとして機能する。そして具体的には、ネットワークの管理会社や、コンピュータのアウトソースを受託するコンピュータセンタ等がその機能を発揮することができる。また配信センタ2は、マイクや映像撮像機を設置した生中継先3等もその管理下におき、音楽や映像など生の情報も提供することが可能である。生中継先からのデータは、リアルタイムにインターネット5を経由して配信しても良いし、ビデオ・オン・デマンドのように、配信センタ2のサーバ(図示せず)に一度格納して、配信要求があるたびに配信しても良い。例えば音楽の生演奏をインターネットを介して配信すれば、同程度の性能を有する再生装置を保有している他の場所でも、生演奏を聴くのと同様の品質で音楽を楽しむことができる。

【0019】図2はこの発明の実施の形態1による再生端末1a, 1b, ... 1nの構成を示した図である。図において、11はマルチメディアデータの配信要求を行う電話機能部、12は配信要求候補となるマルチメディアデータの識別情報を予め記憶する識別情報記憶部で、本再生端末の容量の範囲内でこの識別情報を記憶している。

【0020】また図2において、13は配信されたマルチメディアデータを記憶するデータ記憶部(データ記憶手段)、14はデータ記憶部13に記憶されたマルチメディアデータを再生するデータ再生部(データ再生手段)、15は指定した複数回の繰返し再生を制御する繰返し再生制御部(繰返し再生制御手段)、16はデータ再生部14より1回又は指定した複数回の繰返し再生を終了後、データ記憶部13に記憶されているマルチメディアデータを消滅処理させる消滅処理制御部(消滅処理制御手段)であり、データ記憶部13、データ再生部14、繰返し再生制御部15、消滅処理制御部16は、必要に応じユーザが解体不可能な筐体24に格納しても良い。

【0021】17はデータ再生部14からのデータを増幅し外部出力端子18に出力する増幅部、19はアンテナ、20は本再生端末の入出力を制御する入出力制御部、21は本再生端末の操作を行う操作部、22は電話機能部11のための表示やデータ再生部14により再生されるマルチメディアデータを表示する表示部、23は本再生端末全体の制御を行うCPUである。

【0022】次に再生端末1aのユーザが希望するマルチメディアデータを利用する時の動作について説明する。図3はこのときの動作を示すフローチャートである。図3のステップST1において、再生端末1aのユーザは、希望するマルチメディアデータを識別情報記憶

部12に予め記憶されたマルチメディアデータの識別情報の中から、希望するマルチメディアデータの識別情報を表示部22に表示させながら検索し抽出する。抽出されたこの識別情報に、マルチメディアデータの繰返し再生回数を添付して配信要求情報を作成する。これらの操作は、ユーザが操作部21、表示部22を使用して行う。そして電話機能部11により、上記配信要求情報とこの再生端末1aを特定する契約番号等の認証情報とを、入出力制御部20、アンテナ19を経由し、配信センタ2に送信し希望するマルチメディアデータの配信要求を行う。

【0023】また情報記憶部12にユーザが希望するマルチメディアデータの識別情報がない場合には、ユーザは外部から何らかの方法により希望するマルチメディアデータの識別情報を得て上記処理を行う。

【0024】ステップST2において、配信センタ2は再生端末1aからの配信要求情報と認証情報を受信する。次にステップST3において、配信センタ2は、受信した認証情報から、再生端末1aの契約番号が認証センタ7により認証されているかをチェックする。そして認証されていない再生端末であれば、ステップST4で配信を拒否する。また認証された再生端末であれば、ステップST5で受信した配信要求情報に基づき、配信センタの格納場所から要求されたマルチメディアデータを抽出する。

【0025】そしてステップST6で、配信センタ2は、受信した配信要求情報と認証情報に基づき、送信するマルチメディアデータとその繰返し再生回数に応じた課金処理を行い、ステップST7で金融機関6に対し、料金回収の指示を行う。ステップST6における課金処理の際に、送信するマルチメディアデータとその繰返し再生回数に応じた課金方法以外に、ユーザやその利用度数、利用時間、利用契約に応じた計数処理による課金処理を行っても良い。このような課金処理を行うことにより、ユーザに対し幅広いサービスを提供することが可能となる。

【0026】ステップST8において、ステップST5で抽出したマルチメディアデータ、その繰返し再生回数及び繰返し回数だけ再生後にマルチメディアデータを消滅させる付加情報を含んだ配信情報を再生端末1aに送信する。このとき必要に応じステップST6で算出した課金情報を含ませても良い。

【0027】配信センタ2から送信されたマルチメディアデータ、繰返し再生回数及び付加情報を含んだ配信情報は、ステップST9で再生端末1aのアンテナ19により受信され、入出力制御部20の制御によりデータ記憶部13に記憶される。そしてステップST10で操作部21からの指示に基づき、データ記憶部13に記憶されたマルチメディアデータは、ディジタル/アナログ変換器を内蔵したデータ再生部14により再生され、ディ

ジタル情報からアナログ情報に変換される。そして増幅部17により増幅されて外部出力端子18に出力され、ユーザは送信されたマルチメディアデータを視聴することができる。またデータ再生部14により再生されたマルチメディアデータは、必要に応じ再生端末1aの表示部22に表示される。

【0028】ステップST10においてデータ再生部14によりマルチメディアデータを再生する際、繰返し再生制御部15は、データ記憶部13に記憶されている繰返し回数だけ再生するよう制御を行う。またこのとき消滅処理制御部16は、同様にデータ記憶部13に記憶されている付加情報を理解し、繰返し回数だけ再生後に、ステップST11において、マルチメディアデータを消滅させ、その後のマルチメディアデータの使用を禁止する。

【0029】上記図3の動作フローは、配信センタ2に格納されているマルチメディアデータを利用する時の動作について説明しているが、配信センタ2と契約している生中継先のマルチメディアデータを利用する時の動作についても同様に行える。

【0030】上記ステップST1で、上記再生端末が配信要求情報を配信センタに送信するときに、希望するマルチメディアデータの識別情報とマルチメディアデータの繰返し再生回数を添付して送信しているが、繰返し再生回数を添付せずに、識別情報のみを配信要求情報として送信しても良い。この場合、以降のステップは全て再生回数が1回分として処理される。

【0031】データ記憶部13、データ再生部14、繰返し再生制御部15、消滅処理制御部16は、必要に応じユーザが解体不可能な筐体24に格納しても良い。このような構成にすることにより、受信したデジタルとしての情報をユーザが外部に取り出すことが不可能になる。またユーザが故意に繰返し再生制御部15や消滅処理制御部16を不正に改ざんするのを防いでいる。このようにしてマルチメディアデータの著作権を保護することが可能になる。

【0032】また上記実施の形態では、再生端末1aは、筐体24の内部にデータ記憶部13、データ再生部14、繰返し再生制御部15及び消滅処理制御部16を内蔵しているが、筐体24の部分をこの再生端末とは別の機器とし、この再生端末の制御のもと、この他の機器により上記処理を行っても良い。

【0033】さらに上記実施の形態では、ステップST3で再生端末1aの認証判定を行っているが、認証情報の中に端末の特定とは別にユーザを特定する情報も付加し、ユーザ認証の判定も行うようにすれば、さらに確実な料金回収が可能となる。

【0034】以上のように、この実施の形態1によれば、単なる放送とは異なり、ユーザは要求したマルチメディアデータを使用した再生回数に応じ適正な料金でサ

ービスを受けることが可能となる。またマルチメディアデータをデジタル情報として送受信することで、ユーザは質の高い情報を利用することができる。さらに生中継先のマルチメディアデータのサービスも受けることができ、ユーザは現地にいなくてもタイムリーに生演奏を聴くのと同様の質の高い情報を楽しむことが可能となる。

【0035】またこの実施の形態1によれば、配信センタ2の経営者は、認証センタ7により認証された再生端末のみへの配信サービスを提供することにより、相手を特定でき確実な料金回収が可能となる。さらに配信したマルチメディアデータを再生端末側で利用後に消滅させることにより、配信センタ2の経営者は再利用の場合の料金回収も確実に行うことができる。さらに再生端末側でユーザが不正にデジタル情報として抽出できないようにすることにより、マルチメディアデータの著作権を保護することができる。

【0036】またマルチメディアデータの各保有会社にしてみれば、膨大なデータを保有、管理するよりは、配信センタに保有しているマルチメディアデータを供給した方が効率的な経営を行うことができる。また配信センタは、アーティストと直接に契約し、マルチメディアコンテンツを作成すれば、より安いコストでサービスを提供することができる。

【0037】実施の形態2. インターネットというオープンなネットワークを介しての通信は、そのセキュリティが問題になるが、この実施の形態はユーザのセキュリティの確保と他人による悪用を防ぐために暗号を使用して、マルチメディアデータの配信要求とそれに基づく配信を行うものである。

【0038】図4は再生端末1aと配信センタ2間の通信を、データの暗号化に適した秘密鍵暗号方式と他人の「なりすまし」防止に適した公開鍵暗号方式を併用した方式を模式化した図である。再生端末1aはまずこのマルチメディアデータの配信サービスを受ける契約を行うと、図1における認証センタ7により、公開鍵暗号方式のための公開鍵 $K_{cp}$ と秘密鍵 $K_{ts1}$ の配布を受ける。一方、配信センタ2は、認証センタ7により、公開鍵暗号方式のための公開鍵 $K_{tp1}$ と秘密鍵 $K_{cs}$ の配布を受けている。図1における他の再生端末1b・・・1nは、この契約を行うと、共通の公開鍵 $K_{cp}$ と各再生端末に対応した秘密鍵 $K_{ts2}$ ・・・ $K_{tsn}$ の配布を受け、認証センタ7では、共通の秘密鍵 $K_{cs}$ と各再生端末に対応した公開鍵 $K_{tp2}$ ・・・ $K_{tpn}$ を保有している。また秘密鍵暗号方式では、再生端末1aは鍵として乱数Rを用いて暗号化し、配信センタ2は鍵として乱数R'を用いて暗号化する。

【0039】図5はこの発明の実施の形態2による再生端末1aの構成を示した図である。図において31は暗号化／復号部（暗号化／復号手段）で、再生端末1aが

らの送信内容を暗号化し、配信センタ2からの受信内容を復号化する。また暗号化／復号部31には、認証センタ7により配布された公開鍵暗号方式のための公開鍵 $K_{cp}$ と秘密鍵 $K_{ts1}$ と秘密鍵暗号方式の鍵Rの乱数作成装置が格納されている。暗号化／復号部31以外の構成については、実施の形態1の図2と同じである。さらに暗号化／復号部31は、データ記憶部13、データ再生部14、繰返し再生制御部15、消滅処理制御部16と同様に、必要に応じユーザが解体不可能な筐体24に格納しても良い。

【0040】次に再生端末1aのユーザが希望するマルチメディアデータを利用する時の動作について説明する。全体的な動作フローは実施の形態1における図3と同じであるが、図6及び図8はこの実施の形態2の特有な動作を示すフローチャートであり、図7は再生端末1aが暗号化するときのイメージ図で、図9は配信センタ2が暗号化するときのイメージ図である。

【0041】図6は図3におけるステップST1及びステップST2において、暗号化、復号化の動作を示すフローチャートである。まずステップST1-1において、暗号化／復号部31は、図7に示すように、配信要求を行うマルチメディアデータの識別情報とマルチメディアデータの繰返し再生回数を含んだ配信要求情報を乱数Rの鍵を用いて、MISTY等の秘密鍵暗号方式で暗号化を行う。

【0042】次にステップST1-2において、暗号化／復号部31は、図7に示すように、マルチメディアデータの識別情報を圧縮した識別情報ダイジェストと再生端末1aを特定する契約番号等を含んだ認証情報及びステップST1-1で使用した上記鍵Rを、配信センタ7から配布された公開鍵 $K_{cp}$ を用いて、RSA等の公開鍵暗号方式で暗号化する。ここで、マルチメディアデータの識別情報を圧縮した識別情報ダイジェストは、識別情報のインターネット上での改ざんの有無をチェックするために使用される。暗号化された配信要求情報は、実施の形態1と同様に配信センタ2に送信される。

【0043】次にステップST2-1において、配信要求情報を受信した配信センタ2は、認証センタ7より配布された秘密鍵 $K_{cs}$ を用いて、RSA等の公開鍵暗号方式で復号化し、識別情報ダイジェストと契約番号を含んだ認証情報及び乱数Rの鍵を抽出する。そしてステップST2-2において、抽出した乱数Rの鍵を用いて、識別情報と繰返し再生回数を含んだ配信要求情報を、MISTY等の秘密鍵暗号方式で復号化する。

【0044】次にステップST2-3において、配信センタ2は、ステップST2-1で抽出した識別情報ダイジェストとステップST2-2で抽出した識別情報を比較し、識別情報がインターネット上で改ざんされていないかを判定する。もし比較の結果、両者が異なっていれば、ステップST2-4でマルチメディアデータの配信

を拒否する。

【0045】ステップST2-3において、もし両者が一致し、識別情報がインターネット上で改ざんされていない場合、図3のステップST3に移行する。ステップST3では、ステップST2-1で抽出した契約番号により、実施の形態1と同様に再生端末1aの認証を行う。以後図3におけるステップST7までの動作は、実施の形態1と同様である。

【0046】図8は図3におけるステップST8及びステップST9において、暗号化、復号化の動作を示すフローチャートである。まずステップST8-1において、配信センタ2は、図9に示すように、マルチメディアデータ、その繰返し再生回数及び指定された繰返し回数だけ再生後にマルチメディアデータを消滅させる付加情報を含んだ配信情報を、乱数R'の鍵を用いて、MISTY等の秘密鍵暗号方式で暗号化を行う。

【0047】次にステップST8-2において、配信センタ2は図9に示すように、鍵R'を配信センタ7から配布された公開鍵 $K_{tp1}$ を用いて、RSA等の公開鍵暗号方式で暗号化し、再生端末1aに送信する。

【0048】次にステップST9-1において、暗号化された配信情報を受信した再生端末1aの暗号化／復号部31は、認証センタ7より配布された秘密鍵 $K_{ts1}$ を用いてRSA等の公開鍵暗号方式で復号化し、乱数R'の鍵を抽出する。そしてステップST9-2において、抽出した乱数R'の鍵を用いてMISTY等の秘密鍵暗号方式で復号化し、配信センタ2からのマルチメディアデータ、その繰返し再生回数及び付加情報を含んだ配信情報を得る。以後図3におけるステップST11までの動作は、実施の形態1と同様である。

【0049】また上記実施の形態2では、秘密鍵暗号方式で暗号化する場合、再生端末1aでは鍵R、配信センタ2では鍵R'と別の鍵を使用しているが、再生端末1aと配信センタ2で同じ鍵を使用しても良い。

【0050】以上のように、この実施の形態2によれば、再生端末からの配信要求情報及び配信センタからの配信情報は、秘密鍵暗号方式によりそれぞれ暗号化されて送信されるので、ユーザのインターネット上でのプライバシーを保護することができる。また秘密鍵暗号方式の鍵及び認証情報を公開鍵暗号方式により暗号化しているので、他人の「なりすまし」を防止し易くなり、他人による悪用を防ぐことができる。さらに再生端末から送信されるマルチメディアデータの識別情報を、配信センタでチェックしているので、インターネット上での識別情報の改ざんの有無を知ることができる。

【0051】

【発明の効果】以上のように、請求項1記載の発明によれば、単なる放送とは異なり、ユーザは要求したマルチメディアデータを適正な料金でサービスを受けられるという効果がある。また、配信センタの経営者は、認証セ



ンタにより認証された再生端末のみへの配信サービスを提供することにより、相手を特定でき確実な料金回収が行えるという効果がある。さらに、配信したマルチメディアデータを再生端末側で利用後に消滅させることにより、再利用の場合の料金回収も確実に行えるという効果がある。

【0052】請求項2記載の発明によれば、生中継先のマルチメディアデータのサービスも受けることができ、ユーザは現地にいなくてもタイムリーに生演奏を聴くと同様の質の高い情報を楽しむことができる効果がある。

【0053】請求項3記載の発明によれば、ユーザは要求したマルチメディアデータを希望する回数分再生することができるという効果がある。また、配信センタの経営者は、使用した再生回数に応じ課金することができる効果がある。

【0054】請求項4記載の発明によれば、再生端末と配信センタ間の通信を、暗号を用いて行っているので、ユーザのプライバシーを保護することができる効果がある。

【0055】請求項5記載の発明によれば、再生端末と配信センタ間の通信を、秘密鍵暗号方式と公開鍵暗号方式を併用しているため、適切なデータの暗号化を行えると共に、他人の「なりすまし」を防止できるので、ユーザのプライバシーを保護することができると共に、他人による悪用を防ぐことができる効果がある。

【0056】請求項6記載の発明によれば、再生端末から送信されるマルチメディアデータの識別情報を、配信センタでチェックしているため、インターネット上での識別情報の改ざんの有無を知ることができる効果がある。

【0057】請求項7記載の発明によれば、単なる放送とは異なり、ユーザは要求したマルチメディアデータのサービスを受けられるという効果がある。

【0058】請求項8記載の発明によれば、ユーザは要求したマルチメディアデータを希望する回数分再生することができる効果がある。

【0059】請求項9記載の発明によれば、再生端末と配信センタ間の通信を、暗号を用いて行っているため、

ユーザのプライバシーを保護することができる効果がある。

【0060】請求項10記載の発明によれば、再生端末と配信センタ間の通信を、秘密鍵暗号方式と公開鍵暗号方式を併用しているため、適切なデータの暗号化を行えると共に、他人の「なりすまし」を防止できるので、ユーザのプライバシーを保護することができると共に、他人による悪用を防ぐことができる効果がある。

【0061】請求項11記載の発明によれば、ユーザが不正にデジタル情報として抽出できないようにすることにより、マルチメディアデータの著作権を保護することができる効果がある。

#### 【図面の簡単な説明】

【図1】 この発明の実施の形態1及び2によるマルチメディアデータ配信システムを示す構成図である。

【図2】 この発明の実施の形態1による再生端末の構成図である。

【図3】 この発明の実施の形態1及び2の動作手順を示すフローチャートである。

【図4】 この発明の実施の形態2による暗号方式を模式化した図である。

【図5】 この発明の実施の形態2による再生端末の構成図である。

【図6】 この発明の実施の形態2の動作手順を示すフローチャートである。

【図7】 この発明の実施の形態2の再生端末が暗号化するときのイメージ図である。

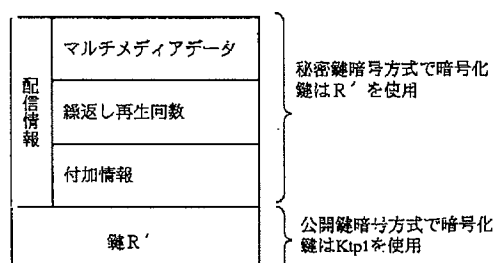
【図8】 この発明の実施の形態2の動作手順を示すフローチャートである。

【図9】 この発明の実施の形態2の配信センタが暗号化するときのイメージ図である。

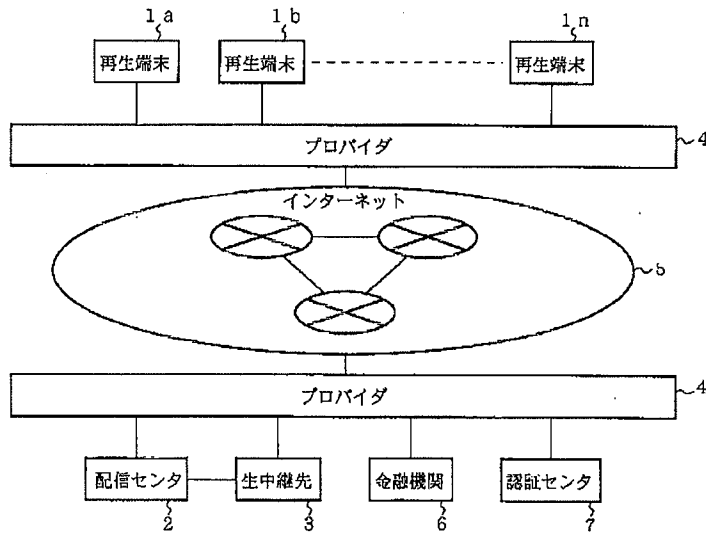
#### 【符号の説明】

1 a, 1 b, . . . 1 n 再生端末、2 配信センタ、3 生中継先、4 プロバイダ、6 金融機関、7 認証センタ、13 データ記憶部（データ記憶手段）、14 データ再生部（データ再生手段）、15 繰返し再生制御部（繰返し再生制御手段）、16 消滅処理制御部（消滅処理制御手段）、31 暗号化／復号部（暗号化／復号手段）。

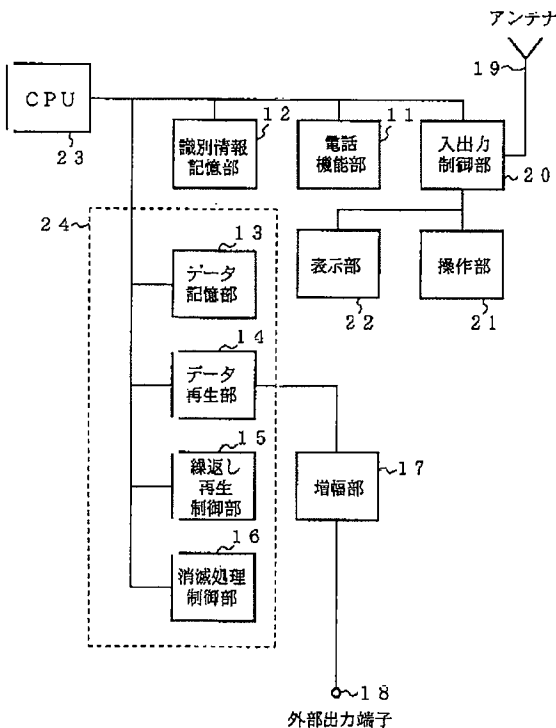
【図9】



【図1】

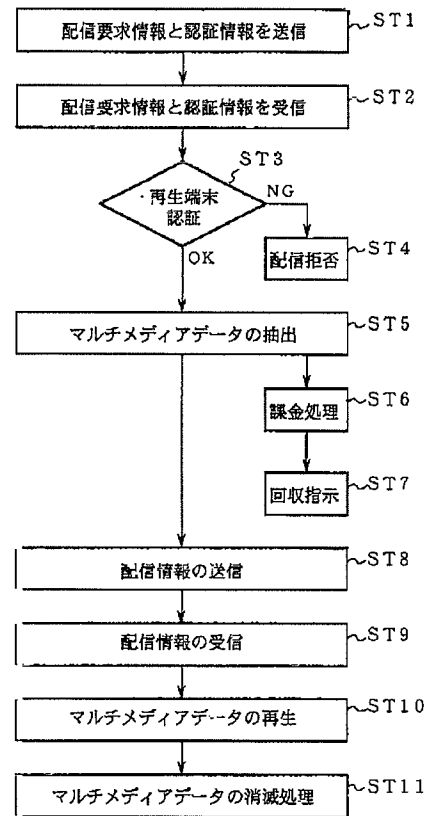


【図2】

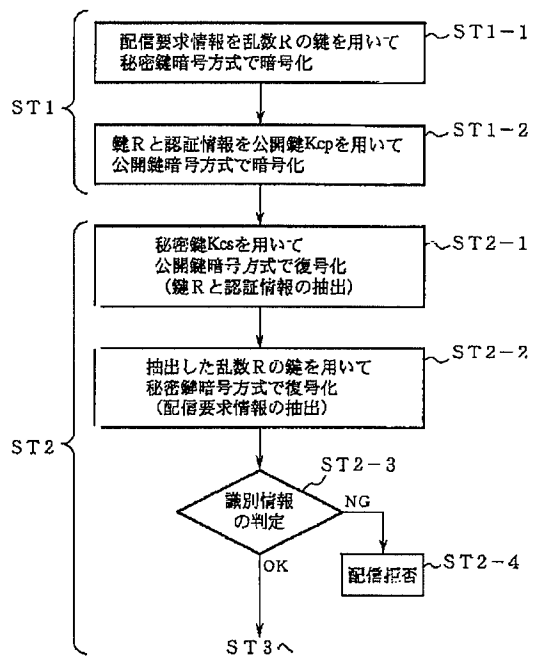


- 13: データ記憶部 (データ記憶手段)  
 14: データ再生部 (データ再生手段)  
 15: 繰返し再生制御部 (繰返し再生制御手段)  
 16: 消滅処理制御部 (消滅処理制御手段)

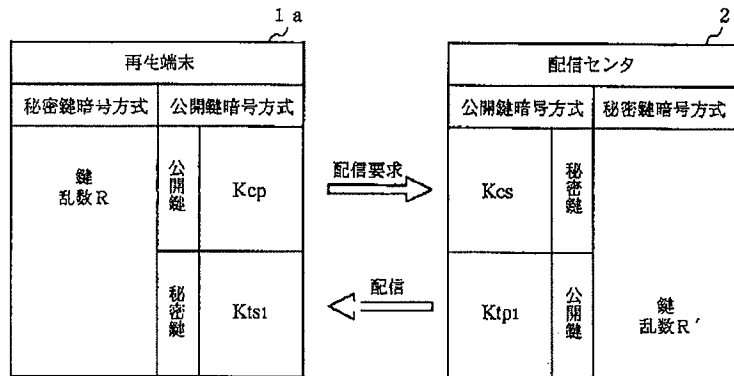
【図3】



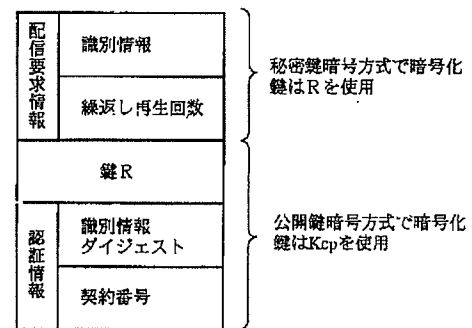
【図6】



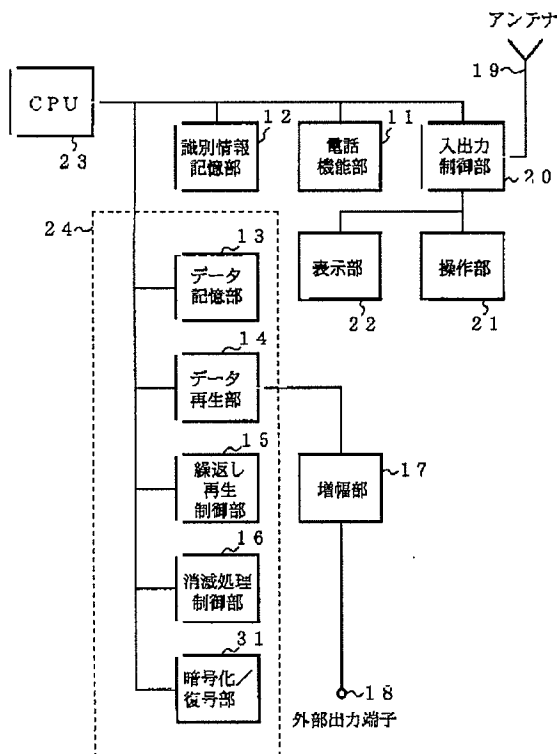
【図4】



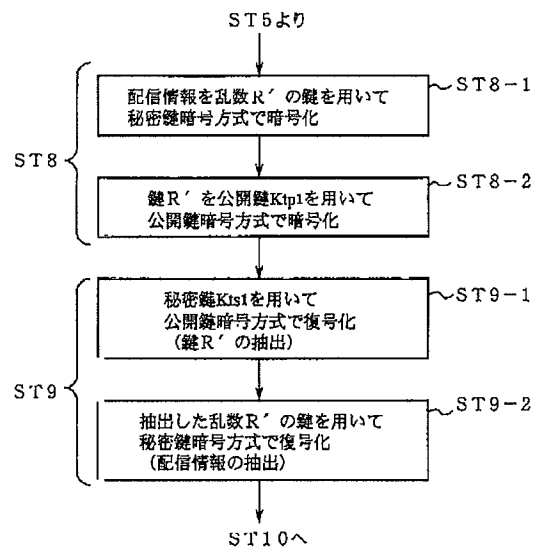
【図7】



【図5】



【図8】



31: 暗号化/復号部 (暗号化/復号手段)

フロントページの続き

(51)Int. Cl.<sup>6</sup>

H04M 15/00

H04N 7/16

識別記号

FI

H04N 7/16

H04L 9/00

C

675D

675B